

AMENDMENTS TO THE CLAIMS

For the convenience of the Examiner, all claims have been presented whether or not an amendment has been made. The claims have been amended as follows:

1. **(Previously Presented)** A method of detecting a computer virus, comprising:
emulating computer executable code in a subject file;
detecting at least one modification to a memory state of a computer system, wherein
the at least one modification:
 is caused by the emulation of the computer executable code; and
 comprises insertion of a pointer to a viral exception handler, the pointer
 associated with a particular exception;
and
detecting at least one instruction, wherein the at least one instruction forces the
particular exception.
2. **(Previously Presented)** The method of Claim 1, wherein:
the at least one modification further comprises installation of the viral exception
handler.
3. **(Previously Presented)** The method of Claim 1, wherein the particular
exception comprises at least one of the following:
 a divide-by-zero arithmetic operation;
 an execution of an undefined computer instruction; and
 a memory access to an undefined or illegal memory address.
4. **(Canceled)**

5. **(Previously Presented)** A method of detecting a computer virus, comprising:
emulating computer executable code in a subject file;
detecting at least one modification to a memory state of a computer system, wherein:
 the memory state comprises a particular interrupt associated with a legitimate
interrupt handler; and
 the at least one modification:
 is caused by the emulation of the computer executable code;
 comprises installation of a viral interrupt handler; and
 associates the particular interrupt with the viral interrupt handler
instead of the legitimate interrupt handler;
and
detecting at least one instruction, wherein the at least one instruction forces the
particular interrupt.
6. **(Previously Presented)** The method of Claim 5, further comprising:
detecting writing of a pointer to at least one predetermined address in a system
memory for storing an interrupt handler pointer.
7. **(Previously Presented)** The method of Claim 5, further comprising:
detecting use of a predetermined instruction to retrieve an address in a system
memory corresponding to an interrupt descriptor table.

8. (Currently Amended) ~~A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method~~ **Logic** for detecting a computer virus, the **logic encoded in computer readable media and operable when executed to** ~~method comprising:~~

emulating **emulate** computer executable code in a subject file;

~~detecting~~ **detect** at least one modification to a memory state of a computer system, wherein the at least one modification:

is caused by the emulation of the computer executable code; and

comprises ~~installation of~~ **insertion of a pointer to** a viral exception handler ~~or a viral interrupt handler~~, **the pointer associated with a particular exception;**

and

~~detecting~~ **detect** at least one instruction, wherein the at least one instruction forces [:] **the particular** ~~an exception associated with the viral exception handler; or an interrupt associated with the viral interrupt handler.~~

9. (Currently Amended) ~~A computer system, comprising~~ Logic for detecting a computer virus, the logic encoded in computer readable media and operable when executed to:

~~a processor; and~~

~~a program storage device readable by a computer system, tangibly embodying a program of instructions executable by the processor to perform a method for detecting a computer virus, the method comprising:~~

~~emulating~~ emulate computer executable code in a subject file;

~~detecting~~ detect at least one modification to a memory state of a computer system, wherein:

the memory state comprises a particular interrupt associated with a legitimate interrupt handler; and

~~the at least one modification:~~

~~is caused by the emulation of the computer executable code; and~~

~~comprises installation of a viral exception handler or a viral interrupt handler; and~~

associates the particular interrupt with the viral interrupt handler instead of the legitimate interrupt handler;

and

detect at least one instruction, wherein the at least one instruction forces the particular interrupt.

10. (Canceled)

11. (Canceled)

12. (Canceled)

13. (Currently Amended) ~~The apparatus of Claim 11, wherein the at least one modification further~~ **An apparatus for detecting computer viruses, comprising:**
an emulator component operable to emulate computer executable code in a subject file; and

a detector component operable to:

detect at least one modification to a memory state of a computer system,
wherein the at least one modification:

is caused by emulation of the computer executable code; and

~~comprises installation of a viral exception handler, and further comprising detecting;~~

and

detect at least one instruction, wherein the at least one instruction forces a particular exception associated with the viral exception handler.

14. (Previously Presented) The apparatus of Claim 13, wherein the particular exception comprises at least one of the following:

a divide-by-zero arithmetic operation;

a memory access to an undefined or illegal memory address; and

execution of an undefined computer instruction.

15. (Previously Presently) The apparatus of Claim 13, wherein the at least one modification further comprises writing of a pointer to the viral exception handler, the pointer associated with the particular exception.

16. **(Currently Amended)** ~~The apparatus of Claim 11, wherein the at least one modification further~~ **An apparatus for detecting computer viruses, comprising:**

an emulator component operable to emulate computer executable code in a subject file; and

a detector component operable to:

detect at least one modification to a memory state of a computer system,
wherein the at least one modification:

is caused by emulation of the computer executable code; and
comprises installation of a viral interrupt handler;

and

detect, ~~and further comprising detecting~~ at least one instruction, wherein the at least one instruction forces a particular interrupt associated with the viral interrupt handler.

17. **(Canceled)**

18. **(Previously Presented)** The apparatus of Claim 16, wherein the at least one modification further comprises writing of a pointer to the viral interrupt handler, the pointer associated with the particular interrupt.

19. **(Previously Presented)** The apparatus of Claim 16, wherein the at least one modification further comprises use of a predetermined instruction to retrieve an address in a system memory corresponding to an interrupt descriptor table.

20. **(Previously Presented)** The method of Claim 1, wherein the computer system comprises a first memory component and a second memory component, and wherein access to the second memory component is more restricted than access to the first memory component.

21. **(Currently Amended)** The method of Claim 20, wherein the viral exception handler ~~or the viral interrupt handler~~ attempts to modify the second memory component.

22. **(New)** The method of Claim 5, wherein the computer system comprises a first memory component and a second memory component, and wherein access to the second memory component is more restricted than access to the first memory component.

23. **(New)** The method of Claim 22, wherein the viral interrupt handler attempts to modify the second memory component.